

Amendment to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (Currently amended) In a distributed computing environment, a method for managing an electronic record for compliance with pre-determined network security rules of an organization, the method comprising:

creating an electronic tag that uniquely identifies the electronic record and that correlates to scripting code, the electronic tag being associated with a deletion prevention specified time period for compliance with the pre-determined network security rules;

storing the at least one electronic tag in a central repository;

sending the electronic record from the distributed computing environment to a recipient, wherein the sending of the electronic record activates the scripting code that correlates to the electronic tag; and

wherein the activated scripting code acts to keep the electronic record from being deleted automatically denying a request to delete the electronic record before expiration of the deletion prevention time period associated with the electronic tag.

Claim 2 (Previously presented) The method of claim 1, further comprising deleting the electronic record and selectively deleting the at least one electronic tag.

Claim 3 (Previously presented) The method of claim 1, further comprising storing the electronic record.

Claim 4 (Canceled)

Claim 5 (Previously presented) The method of claim 1, wherein: the distributed computing environment comprises a computer having a registry and a user profile, and wherein creating the electronic tag comprises generating a reference code and creating the electronic tag at least in part as a function of at least one of the registry, the user profile, and the reference code.

Claim 6 (Previously presented) The method of claim 5, wherein generating the reference code comprises reading the electronic record.

Claim 7 (Previously presented) The method of claim 5, wherein the reference code comprises a classification code and an index code.

Claim 8 (Previously presented) The method of claim 7, wherein the classification code is selected from a group comprising business email, personal email, intramail, bulletin board, minutemail, and purgemail.

Claim 9 (Previously presented) The method of claim 7, wherein the index code identifies the contents of the electronic record and the recipient of the electronic record.

Claim 10 (Previously presented) The method of claim 1, wherein creating the electronic tag comprises:
reading a stored electronic tag; and
generating an electronic tag in response to accessing an electronic record;

Claim 11 (Previously presented) The method of claim 1, wherein the electronic record comprises an email message.

Claim 12 (Previously presented) The method of claim 1, wherein sending the electronic record comprises:
reading the electronic tag; and
generating a new electronic tag at least in part as a function of the read electronic tag, a computer registry, a user profile, and a reference code.

Claim 13 (Currently amended) In a distributed computing environment, an apparatus for managing an electronic record for compliance with a network security rules, the apparatus comprising:

a computer system comprising at least one processor and at least one memory, the computer system being adapted and arranged to create an electronic tag that uniquely

Patent Appl. No. 09/175,589
Attorney Docket No. 150-003 US
Amendment Dated: November 22, 2005
Reply to Office Action Mailed June 2, 2005

identifies the electronic record and that correlates to scripting code, the electronic tag being associated with a deletion prevention time period for compliance with the network security rules;

store the at least one electronic tag in a central repository;
send the electronic record from the distributed computing environment to a recipient, wherein the electronic record, when sent, activates the scripting code that correlates to the electronic tag; and

wherein the scripting code, when activated, acts to keep the electronic record from being deleted automatically deny a request to delete the electronic record before expiration of the deletion prevention time period associated with the electronic tag.

Claim 14 (Previously presented) The apparatus of claim 13, wherein the computer system is further adapted and arranged for purging the electronic record by deleting the electronic record and selectively deleting the at least one electronic tag.

Claim 15 (Canceled)

Claim 16 (Previously presented) The apparatus of claim 13, wherein the distributed computing environment comprises a computer having a registry and a user profile, wherein the computer system is configured and arranged to:

generate a reference code, wherein the electronic tag is generated at least in part as a function of at least one of the registry, the user profile, and the reference code.

Claim 17 (Currently amended) In a distributed computing environment, an article of manufacture for managing an electronic record for compliance with network security rules, the article of manufacture comprising a computer-readable storage medium having a computer program embodied therein that causes the distributed computing environment to:

create an electronic tag that identifies the electronic record and that correlates to scripting code, the electronic tag being associated with a deletion prevention time period for compliance with the network security rules;

store the at least one electronic tag in a central repository;

send the electronic record from the distributed computing environment to a recipient, wherein the electronic record, when sent, activates the scripting code that correlates to the electronic tag; and

wherein the scripting code, when activated, acts to keep the electronic record from being deleted automatically deny a request to delete the electronic record before expiration of the deletion prevention time period associated with the electronic tag.

Claim 18 (Previously presented) The article of claim 17, wherein the computer program further causes the distributed computing environment to purge the electronic record by deleting the electronic record and selectively deleting the at least one electronic tag.

Claim 19 (Previously presented) The article of claim 17, wherein the computer program further causes the distributed computing environment to store the electronic record.

Claim 20 (Canceled)

Claim 21 (Previously presented) The article of claim 17, wherein the distributed computing environment comprises a computer having a registry and a user profile, wherein the computer program further causes the distributed computing environment to generate a reference code, wherein the electronic tag is generated at least in part as a function of at least one of the registry, the user profile, and the reference code.

Claim 22 (Previously presented) The article of claim 17, wherein the computer program further causes the distributed computing environment to:
read a stored electronic tag; and
generate a further electronic tag in response to accessing an electronic record.

Claim 23 (Currently amended) In a distributed computing environment, a method for managing an electronic record for compliance with pre-determined network security rules of an organization, the method comprising:
creating an electronic tag that uniquely identifies the electronic record and that correlates to scripting code, the electronic tag being associated with a deletion prevention specified time period for compliance with the pre-determined network security rules

Patent Appl. No. 09/175,589
Attorney Docket No. 150-003 US
Amendment Dated: November 22, 2005
Reply to Office Action Mailed June 2, 2005

storing the at least one electronic tag in a central repository;
sending the electronic record to a recipient, wherein the sending of the electronic record activates the scripting code that correlates to the electronic tag;
wherein the activated scripting code acts to keep the electronic record from being deleted automatically denying a request to delete the electronic record before expiration of the deletion prevention time period associated with the electronic tag; and
automatically monitoring compliance with the network security rules as a function of the electronic tag.

Claims 24-26 (Canceled)